UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,918	12/12/2001	Louis Guillou	F40.12-0050	3008

7590 02/08/2008

WESTMAN, CHAMPLIN & KELLY P.A.
Suite 1400
900 Second Avenue South
Minneapolis, MN 55402-3319

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
02/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Supplemental ***Notice of Allowability***	**Application No.** 09/889,918	**Applicant(s)** GUILLOU ET AL.	
	Examiner Matthew T. Henning	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the after final amendment filed 10/12/2007*.

2. ☒ The allowed claim(s) is/are *20-26 and 29-41*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☒ All b) ☐ Some* c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☒ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

This action is in response to the communication filed on 10/12/2007.

DETAILED ACTION

Remarks

The examiner notes that the markings indicating changes in claim 20 of the amendment filed 10/12/2007 appear to be mistakenly duplicated from the communication filed 6/7/2007. As such, in order to not further delay the prosecution of this application, the examiner has not held the amendment as non-compliant.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with David Brush on 1/23/2008.

Please replace the current claims with the amended claim listing beginning on the following page:

1-19. (Cancelled)

20. (Previously Presented) A computer implemented process comprising:

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values $G_1, G_2, ..., G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1, ..., m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1, ..., m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, ..., p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a commitment R from a demonstrator, the commitment R having a value computed such that: $R = r^v \bmod n$, wherein r is an integer randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value computed such that: $D = r \bullet Q_1^{d_1} \bullet Q_2^{d_2} \bullet ... \bullet Q_m^{d_m} \bmod n$;and

determining that the demonstrator is authentic if the response D has a value such that: $D^v \bullet G_1^{\varepsilon_1 d_1} \bullet G_2^{\varepsilon_2 d_2} \bullet ... \bullet G_m^{\varepsilon_m d_m} \bmod n$ is equal to the commitment R, wherein, for $i = 1, ..., m$, $\varepsilon_i = +1$ in the case $G_i \bullet Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

21. (Previously Presented) A computer implemented process comprising:

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values $G_1, G_2, ..., G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1, ..., m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1, ..., m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, ..., p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a commitment R from a demonstrator, the commitment R having a value computed using the Chinese remainder method from a series of commitment components R_j, the commitment components R_j having a value such that: $R_j = r_j^v \bmod p_j$ for $j = 1, ..., f$, wherein $r_1, ..., r_f$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \bullet Q_{1,j}^{d_1} \bullet Q_{2,j}^{d_2} \bullet ... \bullet Q_{m,j}^{d_m} \bmod p_j$ for $j = 1, ..., f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for $i = 1, ..., m$ and $j = 1, ..., f$; and determining that the demonstrator is authentic if the response D has a value such that: $D^v \bullet G_1^{\varepsilon_1 d_1} \bullet G_2^{\varepsilon_2 d_2} \bullet \ldots \bullet G_m^{\varepsilon_m d_m} \bmod n$ is equal to the commitment R, wherein, for $i = 1,\ldots,m$, $\varepsilon_i = +1$ in the case $G_i \bullet Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

22. (Previously Presented) A computer implemented process comprising:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, \ldots, p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1,\ldots,m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1,\ldots,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, \ldots, p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a token T from a demonstrator, the token T having a value such that $T = h(M, R)$, wherein h is a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed such that: $R = r^v \bmod n$, wherein r is an integer randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, \ldots, d_m$ randomly;

sending the challenges $d_1, d_2, \ldots, d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value such that: $D = r \bullet Q_1^{d_1} \bullet Q_2^{d_2} \bullet \ldots \bullet Q_m^{d_m} \bmod n$; and

determining that the message M is authentic if the response D has a value such that: $h\left(M, D^v \bullet G_1^{\varepsilon_1 d_1} \bullet G_2^{\varepsilon_2 d_2} \bullet \ldots \bullet G_m^{\varepsilon_m d_m} \bmod n\right)$is equal to the token T , wherein, for $i = 1,\ldots,m$, $\varepsilon_i = +1$ in the case $G_i \bullet Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

23. (Previously Presented) A computer implemented process comprising:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, \ldots, p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1,\ldots,m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1,\ldots,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, \ldots, p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a token T from a demonstrator, the token T having a value such that $T = h(M, R)$, wherein h is a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed out of commitment components R_j by using the Chinese remainder method, the commitment components R_j having a value such that: $R_j = r_j^v \bmod p_j$ for $j = 1,\ldots,f$, wherein $r_1, \ldots, r_f$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, \ldots, d_m$ randomly;

sending the challenges $d_1, d_2, \ldots, d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \bullet Q_{1,j}{}^{d_1} \bullet Q_{2,j}{}^{d_2} \bullet \ldots \bullet Q_{m,j}{}^{d_m} \bmod p_j$ for $j = 1, \ldots, f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for $i = 1, \ldots, m$ and $j = 1, \ldots, f$; and

determining that the message M is authentic if the response D has a value such that: $h(M, D^v \bullet G_1{}^{\varepsilon_1 d_1} \bullet G_2{}^{\varepsilon_2 d_2} \bullet \ldots \bullet G_m{}^{\varepsilon_m d_m} \bmod n)$ is equal to the token T, wherein, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ in the case $G_i \bullet Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

24. (Previously Presented) The computer implemented process according to claim 20, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, \ldots, m$.

25. (Previously Presented) A computer implemented process comprising:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, \ldots, p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1,...,m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1,...,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1,..., p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

recording a message M to be signed;

choosing m integers r_i randomly, wherein i is an integer between 1 and m;

computing commitments R_i having a value such that: $R_i = r_i^v \bmod n$ for $i = 1,...,m$;

computing a token T having a value such that $T = h(M, R_1, R_2,..., R_m)$, wherein h is a hash function producing a binary train consisting of m bits;

identifying the bits $d_1, d_2,..., d_m$ of the token T;

computing responses $D_i = r_i \cdot Q_i^{d_i} \bmod n$ for $i = 1,...,m$; and

performing at least one of transmitting the token T and the response Di to at least one verifying entity, or storing the token T and the response Di on a database accessible to the public or to at least one verifying entity.

26. (Previously Presented) The computer implemented process according to claim 25, further comprising:

collecting the token T and the responses D_i for $i = 1,...,m$; and

determining that the message M is authentic if the responses D_i have a value such that:

$$h\left(M, D_i^{\ v} \cdot G_1^{\ \varepsilon_1 d_1} \bmod \underline{n}, D_2^{\ v} \cdot G_2^{\ \varepsilon_2 d_2} \bmod n, \ldots, D_m^{\ v} \cdot G_m^{\ \varepsilon_m d_m} \bmod n\right)$$

is equal to the token T, wherein, for $i = 1,\ldots,m$, $\varepsilon_i = +1$ in the case $G_i \cdot Q_i^{\ v} = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^{\ v} \bmod n$.

27. (Cancelled)

28. (Cancelled)

29. (Previously Presented) The computer implemented process according to claim 21, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1,\ldots,m$.

30. (Previously Presented) The computer implemented process according to claim 22, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1,\ldots,m$.

31. (Previously Presented) The computer implemented process according to claim 23, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1,\ldots,m$.

32. (Currently Amended) A ~~computer readable medium~~ memory storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^{\ v} \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^{\ v} \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1,...,p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1,...,m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1,...,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1,...,p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a commitment R from a demonstrator, the commitment R having a value computed such that: $R = r^v \bmod n$, wherein r is an integer randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value computed such that: $D = r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot ... \cdot Q_m^{d_m} \bmod n$; and

determining that the demonstrator is authentic if the response D has a value such that: $D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot ... \cdot G_m^{\varepsilon_m d_m} \bmod n$ is equal to the commitment R, wherein, for $i = 1,...,m$, $\varepsilon_i = +1$ in the case $G_i \cdot Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

33. (Currently Amended) A ~~computer readable medium~~ memory storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values

$G_1, G_2, ..., G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1, ..., m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1, ..., m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, ..., p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a commitment R from a demonstrator, the commitment R having a value computed using the Chinese remainder method from a series of commitment components R_j, the commitment components R_j having a value such that: $R_j = r_j^v \bmod p_j$ for $j = 1, ..., f$, wherein $r_1, ..., r_f$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \cdot Q_{1,j}^{d_1} \cdot Q_{2,j}^{d_2} \cdot ... \cdot Q_{m,j}^{d_m} \bmod p_j$ for $j = 1, ..., f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for $i = 1, ..., m$ and $j = 1, ..., f$; and

determining that the demonstrator is authentic if the response D has a value such that: $D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot ... \cdot G_m^{\varepsilon_m d_m} \bmod n$ is equal to the commitment R, wherein, for $i = 1, ..., m$,

$\varepsilon_i = +1$ in the case $G_i \cdot Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

34. (Currently Amended) A ~~computer readable medium~~ memory storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, \ldots, p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1, \ldots, m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1, \ldots, m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, \ldots, p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a token T from a demonstrator, the token T having a value such that $T = h(M, R)$, wherein h is a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed such that: $R = r^v \bmod n$, wherein r is an integer randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, \ldots, d_m$ randomly;

sending the challenges $d_1, d_2, \ldots, d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value such that: $D = r \cdot Q_1^{d_1} Q_2^{d_2} \cdot \ldots \cdot Q_m^{d_m} \bmod n$; and determining that the message M is authentic if the response D has a value such that: $h\left(M, D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot \ldots \cdot G_m^{\varepsilon_m d_m} \bmod n\right)$ is equal to the token T, wherein, for $i = 1,\ldots,m$, $\varepsilon_i = +1$ in the case $G_i \cdot Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

35. (Currently Amended) A ~~computer readable medium~~ memory storing instructions which when executed cause a processor to execute the following method:
obtaining a set of one or more private values $Q_1, Q_2,\ldots, Q_m$ and respective public values $G_1, G_2,\ldots, G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1,\ldots, p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1,\ldots,m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1,\ldots,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1,\ldots, p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a token T from a demonstrator, the token T having a value such that $T = h(M, R)$, wherein h is a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed out of commitment components R_j by using the Chinese remainder method, the commitment components R_j having a value such that: $R_j = r_j^v \bmod p_j$ for $j = 1,\ldots, f$, wherein $r_1,\ldots, r_f$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2,\ldots, d_m$ randomly;

sending the challenges $d_1, d_2, \ldots, d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \cdot Q_{1,j}{}^{d_1} \cdot Q_{2,j}{}^{d_2} \cdot \ldots \cdot Q_{m,j}{}^{d_m} \bmod p_j$ for $j = 1, \ldots, f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for $i = 1, \ldots, m$ and $j = 1, \ldots, f$; and

determining that the message M is authentic if the response D has a value such that: $h\left(M, D^v \cdot G_1{}^{\varepsilon_1 d_1} \cdot G_2{}^{\varepsilon_2 d_2} \cdot \ldots \cdot G_m{}^{\varepsilon_m d_m} \bmod n\right)$ is equal to the token T, wherein, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ in the case $G_i \cdot Q_i{}^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i{}^v \bmod n$.

36. (Currently Amended) The ~~computer readable medium~~ memory according to claim 32, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, \ldots, m$.

37. (Currently Amended) The ~~computer readable medium~~ memory according to claim 33, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, \ldots, m$.

38. (Currently Amended) The ~~computer readable medium~~ memory according to claim 34, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, \ldots, m$.

39. (Currently Amended) The ~~computer readable medium~~ memory according to claim 35, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, \ldots, m$.

40. (Currently Amended) A ~~computer readable medium~~ memory storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i{}^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i{}^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1,\ldots,p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v=2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i=1,\ldots,m$ is such that $G_i \equiv g_i^{\;2} \bmod n$, wherein g_i for $i=1,\ldots,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1,\ldots,p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

recording a message M to be signed;

choosing m integers r_i randomly, wherein i is an integer between 1 and m;

computing commitments R_i having a value such that: $R_i = r_i^{\,v} \bmod n$ for $i=1,\ldots,m$;

computing a token T having a value such that $T=h(M,R_1,R_2,\ldots,R_m)$, wherein h is a hash function producing a binary train consisting of m bits;

identifying the bits $d_1,d_2,\ldots,d_m$ of the token T;

computing responses $D_i = r_i \cdot Q_i^{\,d_i} \bmod n$ for $i=1,\ldots,m$; and

performing at least one of transmitting the token T and the response Di to at least one verifying entity, or storing the token T and the response Di on a database accessible to the public or to at least one verifying entity.

41. (Currently Amended) The ~~computer readable medium~~ memory according to claim 40, the method further comprising:

collecting the token T and the responses D_i for $i=1,\ldots,m$; and determining that the message M is authentic if the responses D_i have a value such that:

$$h\left(M, D_i^{\ v} \cdot G_1^{\ \varepsilon_1 d_1} \bmod n, D_2^{\ v} \cdot G_2^{\ \varepsilon_2 d_2} \bmod n, \ldots, D_m^{\ v} \cdot G_m^{\ \varepsilon_m d_m} \bmod n\right)$$

is equal to the token T, wherein, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ in the case $G_i \cdot Q_i^{\ v} = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^{\ v} \bmod n$.

Allowable Subject Matter

Claims 20-26, and 29-41 are allowed.

The reasons for indicating allowable subject matter are the same as those provided in the office action dated 5/3/2005.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew Henning/
Assistant Examiner
Art Unit 2131
2/1/2008

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100